

The present invention relates to a method for the identification of a person and a portable device enabling implementation of the method.

5 It applies in particular, but not exclusively, to the production of identity documents, such as passports and identity cards, giving various data enabling a person to be identified. These data generally comprise data on the civil status of the person as well as a black-and-white or colour identity photograph and optionally anthropometric data and the fingerprint of the index finger of one hand.

10 Identity documents are currently produced by printing on a paper, board or plasticised support. Despite all the precautions taken, such as the use of special papers, it proves possible to forge them using relatively modest means and relatively easy access.

15 The aim of the present invention is to eliminate these disadvantages. To this end it proposes a method for the secure identification of a person, comprising affixing identification data on the person on an identification support of the paper type, assigned to the person, and reading these data.

According to the invention, this method is characterised in that it comprises:

- fixing on the identification support a thin electronic chip comprising memory means and contactless transmission means and reception means for transmitting the data stored and for receiving the data to be stored, respectively, by the memory means,
 - 5 - digitising and then encrypting the data affixed to the identification support,
 - transmission of the encrypted data to the receiving means and storing thereof by the memory means, and
 - 10 - on each identification of the person, reception by the read means of the data stored by the memory means of the electronic chip fixed on the identification support assigned to the person, decryption of these data and comparison of these data with the data affixed to the identification support.
- 15 The method according to the invention thus makes it possible, by simple comparison of the data stored in the chip and the data appearing on the identification support, to detect any forging of the latter. Moreover, it implements an electronic chip of advanced technology; it is thus not possible to manufacture or forge it with the aid of current means, such as printing means. The invention thus makes it possible to identify a person with high
- 20 security.

Advantageously, the identification data stored in the electronic chip comprise the digitised image of an identity photograph or of a fingerprint, this digitised image being processed by an image compression algorithm before being encrypted.

25

Thus, access to the electronic chip, both when writing and when reading, implies knowledge at one and the same time of the encryption algorithm and the image compression algorithm used.

30

According to a special feature of the invention, the data are stored by memory means of the electronic chip in accordance with a predefined structure which must be known in order to read the data that are stored in said means.

As mentioned above, the present invention also relates to an identification device enabling implementation of the method, this device comprising a thin support made of paper, board or plastic material, an electronic chip of the contactless type in which transmission means of the transponder type and memory means coupled to the transmission means are
5 integrated, the transmission means comprising connection means for connecting to a transmission antenna, the thickness of the chip being very small so as to be able to be incorporated in the support without allowing significant excessive thickness to arise.

Advantageously, the antenna is in the form of a coil, the turns of which are screen printed
10 on the sheet of board, the chip being fixed on the sheet of paper by soldering connection means to the connection terminals of the antenna.

In this way the connection of the chip to the transmission antenna ensures fixing of the chip on the sheet at the same time.

15 One embodiment of the device according to the invention will be described below, by way of non-limiting example, with reference to the appended drawings, in which

Figure 1 shows a system enabling implementation of the method according to
20 the invention;

Figures 2 and 3, show, in the form of block diagrams, the chain of the various steps of the method according to the invention;

25 Figure 4 shows an electronic chip used for implementation of the method according to the invention.

The method according to the invention makes it possible to produce an identification device for a person, this device being in the form of a support made of paper or board, or a
30 badge made of plastic material, to which a photograph and/or a fingerprint are affixed and on which identification data on the person are printed. A transponder chip, which will be described below with reference to Figure 4, comprising computation means, such as a microprocessor core, a memory and contactless means for transmission and reception of

data, is incorporated in this support.

Figure 1 shows a system enabling implementation of the method according to the invention, comprising a computer 1 connected to capture means 4, such as a keyboard, to a display screen 3, a printer 6, an image digitisation device 2, such as a scanner, and a read device 7 for transponder chips, for example of the contactless type.

When the system does not serve merely to perform identify checks, but must enable the production of an identification support according to the method according to the invention, the read device 7 comprises write means enabling data to be transmitted to the transponder chip incorporated in the identification support.

Figure 2 illustrates the various steps enabling the production of an identification device according to the invention.

15

The method according to the invention uses, for example, an image 8 enabling a person to be identified, such as an identity photograph and/or a fingerprint. In the first step 11, this image is first of all digitised by means of a digitisation device 2. The digitised image obtained is then subjected in step 12 to a compression process which, without significantly altering the quality of the image, enables the latter to be stored in a digital memory of relatively low capacity. By virtue of current image compression techniques it is possible to store an identity photograph in several hundred bytes, with little loss of image quality.

In parallel, the identification data 9 relating to the person, such as the data on the civil status (name, first name, date and place of birth, ...) and anthropometric data (sex, height, eye colour, ...) are input into the computer 1 (step 16), which combines and organises these data with the image data in accordance with a pre-established sequence (step 13) and applies an encryption algorithm to them (step 14). The data organised and encrypted in this way are then transmitted to the chip 30 incorporated in an identification support 10, for storing in the latter. Furthermore, the data 9 input in step 11 are printed on the support 10 (step 17).

It should be noted that step 14 can be carried out before step 13, which, depending on the

encryption algorithm used, can make access to the data stored by the chip 30 even more difficult.

Figure 3 shows the operations carried out during an identity check on a person possessing an identification support 10.

In step 22 the read device 7 requests the transfer of the data stored in the transponder chip 30. These data are then transmitted to the computer 1 for decrypting in the latter (step 23) and analysed so as to separate the identification data from the data relating to the digitised image. The image data are decompressed (step 24), then displayed on the display screen 3 with the identification data (step 26), the operator carrying out the identity check is then able to verify that the printed data and the photograph appearing on the identification support 10 do correspond to those displayed on the screen 3.

According to a special feature of the invention, the encryption algorithm used is of the encryption key type, the key chosen being the serial number of the chip 30, which is unique and which is stored in an inalterable manner by the memory means of the latter. The encryption 14 and decryption 23 steps then comprise an operation that precedes reading of the serial number of the chip with the aid of the read means 7.

20

Furthermore, it is possible to provide for automation of the verification operations by digitising the photograph 8 affixed to the support 10 and the data that are printed thereon with the aid of the scanner 2 and by processing the latter by means of character recognition software (step 21). It then suffices to perform step 27, comparison of the data read on the chip 30 and the data resulting from the digitisation, and to indicate on the display screen 3 whether differences have been detected.

25

In parallel, the data, including the image data read in the transponder chip 30, can be compared with the identification data for persons sought, stored in a database 41 accessible to the computer 1.

30

In Figure 4, the transponder chip 30 comprises a memory module 34 and a transmission module 32, the transmission module being connected by connection means 35 to an

antenna 33. The unit comprising the memory and transmission modules can be fixed on a very thin support 31, for example made of paper. Thus, in the case of a transponder chip with a memory capacity of 16 kbits, the unit does not exceed a few tens of millimetres in thickness. Such a capacity is perfectly compatible with the size of the digital image to be stored, taking account of current performances of image compression techniques.

As mentioned above, the chip 30 contains a microprocessor used to manage and control data transfers between the memory 34 and the read/write device 7. The microprocessor can thus assign one or more access keys to the unit or to certain parts of the memory 34 and completely block access to the chip after a certain predefined number of access attempts with the aid of an incorrect key. In this way it is not possible for an unauthorised person to copy the contents of a chip and transfer these to another chip.

The microprocessor of the chip 30 is also programmed to manage collisions, that is to say simultaneous transmissions between a reader and several chips.

Moreover, in the case of induction chips, the transmission antenna 33 is in the form of a coil which enables the read and/or write device 7 to supply energy by induction to the chip 30, the magnetic field applied to the coil being modulated in order to effect data transmission.

The transponder chip used by the invention advantageously uses a transmission frequency of a few MHz, such that the coil 33 has only a few turns, which can be formed on the support by a simple printing process or screen printing, the connection means 35 being in the form of microspheres deposited directly on the silicon substrate of the chip, which are soldered to the connection pins of the antenna, which are also produced by printing or screen printing, the connection to the antenna at the same time ensuring that the chip is held on the support 10. It is also possible to make provision for gluing a sheet of paper on the support 10 so as to cover and mask the other face of the chip 30 and the antenna 33.

Alternatively, the chip and its support, as well as the printed or screen printed antenna can be installed as a sandwich between two pieces of ordinary paper or paper with security features.

It should be noted that such a transmission frequency makes it possible to obtain a relatively high transmission rate, which enables virtually instantaneous reading of the data stored by the chip to be achieved.

WHAT IS CLAIMED IS:

1. A method for the secure identification of a person, comprising affixing identification data on the person on a thin identification support of the board or plastic material type, assigned to the person, and reading these data, characterised in that it comprises:

- fixing on the identification support (10) a thin electronic chip (30) comprising memory means (34) and contactless transmission means and reception means (32) for transmitting the data stored and for receiving the data to be stored, respectively, by the memory means,
- digitising (11, 16) and then encrypting (14) the data affixed to the identification support (10),
- contactless transmission (15) of the encrypted data to the receiving means (32) and storing thereof by the memory means (34), and
- on each identification of the person, reception (22) by the read means (7) of the data stored by the memory means (34) of the electronic chip (30) fixed on the identification support (10) assigned to the person, decryption (23) of these data and comparison (27) of these data with the data affixed to the identification support.

2. The method as claimed in Claim 1, wherein the identification data stored in the electronic chip (30) comprise the digitised image of an identity photograph (8) and/or of a fingerprint, the method also comprising processing (12) of the digitised image by an image compression algorithm before its encryption (14).

3. The method as claimed in Claims 1 or 2, wherein, before encryption (14) of the identification data, it comprises a step for reading a serial number of the chip stored in an inalterable manner by the memory means (34), this serial number being unique, and the use of this serial number as encryption key, and prior reading of this serial number during the decryption (23) of the data stored by the chip.

4. The method as claimed in one of the preceding claims, wherein during the identification of a person it comprises the digitisation (21) of the data

affixed to the support and comparison, by a computer (1), of these data with those originating from the chip incorporated in the support.

5 5. The method as claimed in one of the preceding claims,
wherein, during the identification of a person, it comprises comparison of the data read
with a set of identification data on persons sought stored in a database (41).

10 6. The method as claimed in one of the preceding claims,
wherein the identification data are stored on the chip (30) in accordance with a predefined
structure which must be known in order to be able to read these data.

7. A device for identifying a person for implementing the method as claimed
in one of the preceding claims,
wherein it comprises a thin support (10) made of paper or plastic material, a contactless
15 electronic chip (30) in which contactless transmission and reception (32) means of the
transponder type and memory means (34) coupled to the transmission and reception means
and in which the data for identification of the person are stored are integrated, the
transmission and reception means comprising connection means (35) for connecting to a
transmission antenna (33), the thickness of the chip being very small so as to be able to be
20 incorporated in the support without allowing significant excessive thickness to arise.

8. The device as claimed in Claim 7,
wherein the chip (30) is of the induction type, the transmission antenna (33) being in the
form of a coil which enables the read and/or write device (7) to supply the chip (30) with
25 power by induction, the magnetic field applied to the coil being modulated in order to
effect transmission of the data.

9. The device as claimed in Claim 7 or 8,
wherein the chip (30) advantageously uses a transmission frequency of a few MHz, such
30 that the coil (33) has only a few turns which are formed on the support by a printing
process, the connection means (35) being in the form of microspheres which are integral
with the chip and are soldered onto the connection terminals of the antenna, which are also
produced by a printing process, the connection to the antenna at the same time ensuring

that the chip is held on the support (10).

10. The device as claimed in one of Claims 7 to 9,
wherein the chip (30) has computation means which authorise access to all or part of the
5 memory means (34) only if the transmission and reception (32) means receive a
corresponding predetermined key.

11. The device as claimed in one of Claims 7 to 10,
wherein the chip (30) and the printed antenna are installed as a sandwich between two
10 sheets of ordinary paper or paper with security features.

LEGEND FOR FIGURES

- 1 = Computer
- 7 = Reader
- 5 11 = Digitisation
- 13 = Data organisation
- 14 = Encryption
- 17 = Printing
- 21 = Digitisation
- 10 22 = Reading
- 23 = Decryption
- 24 = Decompression
- 26 = Display
- 27 = Comparison

①9 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

①1 N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 776 153

②1 N° d'enregistrement national :

98 03096

⑤1 Int Cl⁶ : H 04 L 9/12

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 10.03.98.

③0 Priorité :

⑦1 Demandeur(s) : **ORDICAM RECHERCHE ET DEVELOPPEMENT Société anonyme — FR.**

⑦2 Inventeur(s) : **MICHOT GERARD.**

④3 Date de mise à la disposition du public de la demande : 17.09.99 Bulletin 99/37.

⑤6 Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

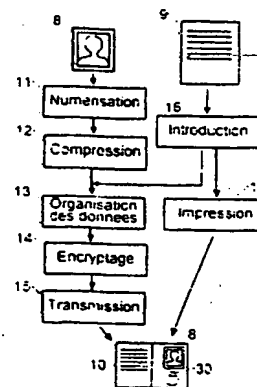
⑥0 Références à d'autres documents nationaux apparentés :

⑦3 Titulaire(s) :

⑦4 Mandataire(s) : **CABINET MOUTARD.**

⑤4 **PROCEDE POUR L'IDENTIFICATION SECURITAIRE D'UNE PERSONNE ET DISPOSITIF PORTATIF POUR LA MISE EN OEUVRE DU PROCEDE.**

⑤7 Ce procédé comprend l'apposition sur un support d'identification (10) en papier ou en matière plastique de faible épaisseur, attribué à une personne, d'informations d'identification de celle-ci, la fixation sur le support (10) d'une puce électronique (30) de faible épaisseur, comprenant une mémoire et un émetteur-récepteur sans contact, respectivement pour transmettre les informations stockées et pour recevoir les informations à stocker dans la mémoire, la numérisation (11, 16), puis l'encryptage (14) des informations apposées sur le support d'identification (10), la transmission (15) sans contact des informations encryptées vers l'émetteur-récepteur et leur stockage dans la mémoire, et à chaque identification de la personne, la réception par un lecteur des informations stockées dans la mémoire de la puce (30) fixée sur le support (10) attribué à la personne, le dé-encryptage de ces informations, et leur comparaison avec les informations apposées sur le support (10).



FR 2 776 153 - A1



La présente invention concerne un procédé pour l'identification d'une personne et un dispositif portatif permettant la mise en oeuvre du procédé.

Elle s'applique notamment, mais non exclusivement, à la réalisation de pièces
5 d'identité, telles que les passeports et les cartes d'identité, donnant différentes informations permettant d'identifier une personne. Ces informations comprennent généralement les informations d'état civil de la personne, ainsi qu'une photographie d'identité en noir et blanc ou en couleurs, et éventuellement des informations anthropométriques et l'empreinte digitale de l'index d'une main.

10

Les pièces d'identité sont à l'heure actuelle réalisées par impression sur un support papier, papier cartonné ou plastifié. Malgré toutes les précautions prises, telles que l'emploi de papiers spéciaux, il s'avère possible de les falsifier en utilisant des moyens relativement modestes et d'un accès relativement aisé.

15

La présente invention a pour but de supprimer ces inconvénients. A cet effet, elle propose un procédé pour l'identification sécuritaire d'une personne, comprenant l'apposition sur un support d'identification du type en papier, attribué à la personne, d'informations d'identification de la personne, et la lecture de ces
20 informations.

Selon l'invention, ce procédé est caractérisé en ce qu'il comprend :

- 5 - la fixation sur le support d'identification d'une puce électronique de faible épaisseur, comprenant des moyens de mémorisation et des moyens d'émission et de réception, sans contact, respectivement pour transmettre les informations stockées et pour recevoir les informations à stocker par les moyens de mémorisation,
- 10 - la numérisation, puis l'encryptage des informations apposées sur le support d'identification,
- 15 - la transmission des informations encryptées vers les moyens de réception et leur stockage par les moyens de mémorisation, et
- 20 - à chaque identification de la personne, la réception par des moyens de lecture des informations stockées par les moyens de mémorisation de la puce électronique fixée sur le support d'identification attribué à la personne, le décryptage de ces informations, et la comparaison de ces informations avec les informations apposées sur le support d'identification.
- 25 Le procédé selon l'invention permet ainsi, par simple comparaison entre les informations stockées dans la puce et les informations apparaissant sur le support d'identification, de détecter toute falsification de celui-ci. Par ailleurs, il met en oeuvre une puce électronique de technologie évoluée ; il n'est donc pas possible de le fabriquer ou falsifier à l'aide de moyens courants, tels que des moyens d'impression. L'invention permet ainsi d'identifier une personne avec une grande sécurité.

30 Avantageusement, les informations d'identification stockées dans la puce électronique comprennent l'image numérisée d'une photographie d'identité ou d'une empreinte digitale, cette image numérisée étant traitée avant d'être encryptée par un algorithme de compression d'image.

35 Ainsi, l'accès à la puce électronique aussi bien en écriture qu'en lecture, implique que l'on connaisse à la fois l'algorithme d'encryptage, et l'algorithme de compression d'images utilisé.

 Selon une particularité de l'invention, les informations sont stockées par les moyens de mémorisation de la puce électronique selon une organisation

prédéfinie qu'il est nécessaire de connaître pour lire les informations qui y sont stockées.

Comme précédemment mentionné, la présente invention concerne également un
5 dispositif d'identification permettant la mise en oeuvre du procédé, ce dispositif
comprenant un support en papier, papier cartonné ou matière plastique de faible
épaisseur, une puce électronique du type sans contact dans laquelle sont intégrés
des moyens de transmission du type transpondeur et des moyens de mémorisation
10 couplés aux moyens de transmission, les moyens de transmission comprenant des
moyens de connexion pour se connecter à une antenne de transmission,
l'épaisseur de la puce étant très faible de manière à pouvoir être incorporée au
support sans laisser apparaître une surépaisseur importante.

Avantageusement, l'antenne présente la forme d'une bobine dont les spires sont
15 sérigraphiées sur la feuille de papier cartonné, la puce étant fixée sur la feuille de
papier par soudage des moyens de connexion sur les bornes de connexion de
l'antenne.

De cette manière, la connexion de la puce à l'antenne de transmission assure en
20 même temps la fixation de la puce sur la feuille.

Un mode de réalisation du dispositif selon l'invention sera décrit ci-après, à titre
d'exemple non limitatif, avec référence aux dessins annexés dans lesquels

25 La figure 1 représente un système permettant la mise en oeuvre du
procédé selon l'invention ;

Les figures 2 et 3 représentent sous la forme de schémas bloc,
l'enchaînement des différentes étapes du procédé selon l'invention ;

30 La figure 4 représente une puce électronique utilisée pour la mise
en oeuvre du procédé selon l'invention.

Le procédé selon l'invention permet de réaliser un dispositif d'identification d'une
personne, ce dispositif se présentant sous la forme d'un support en papier, papier
cartonné, ou badge en matière plastique sur lequel sont apposées une
photographie et/ou une empreinte digitale, et sur lequel sont imprimées des
35 informations d'identification de la personne. Dans ce support est incorporée une

puce transpondeur qui sera décrite ultérieurement en référence à la figure 4, comprenant des moyens de calcul tel qu'un coeur de microprocesseur, une mémoire et des moyens sans contact d'émission et de réception d'informations.

5 La figure 1 représente un système permettant la mise en oeuvre du procédé selon l'invention comprenant un calculateur 1 connecté à des moyens de saisie 4 tels qu'un clavier, à un écran de visualisation 3, une imprimante 6, un dispositif de numérisation d'images 2, tel qu'un scanner, et un dispositif de lecture 7 de puces transpondeur, par exemple de type sans contact.

10 Lorsque le système ne sert pas simplement à effectuer des contrôles d'identité, mais doit permettre de réaliser un support d'identification conformément au procédé selon l'invention, le dispositif de lecture 7 comporte des moyens d'écriture permettant de transmettre des informations à la puce transpondeur
15 incorporée dans le support d'identification.

La figure 2 illustre les différentes étapes permettant de réaliser un dispositif d'identification selon l'invention.

20 Le procédé selon l'invention utilise par exemple une image 8 permettant d'identifier une personne, telle qu'une photographie d'identité et/ou une empreinte digitale. A la première étape 11, cette image est tout d'abord numérisée au moyen du dispositif de numérisation 2. L'image numérisée obtenue subit ensuite à l'étape 12 un traitement de compression qui, sans altérer d'une manière importante la
25 qualité de l'image, lui permet d'être stockée dans une mémoire numérique de relativement faible capacité.

Grâce aux techniques actuelles de compression d'image, il est possible de stocker une photographie d'identité sur quelques centaines d'octets, avec une faible perte de qualité d'image.

30 Parallèlement, les informations d'identification 9 concernant la personne, telles que des informations d'état civil (nom, prénom, date et lieu de naissance, ...) et anthropométriques (sexe, taille, couleur des yeux, ...) sont introduites dans le calculateur 1 (étape 16), lequel combine et organise ces informations avec les
35 informations d'image selon un ordre préétabli (étape 13), et leur applique un algorithme d'encryptage (étape 14). Les données ainsi organisées et encryptées sont ensuite transmises à la puce 30 incorporée à un support d'identification 10,

pour y être stockées. Par ailleurs, les informations 9 introduites à l'étape 11 sont imprimées sur le support 10 (étape 17).

Il est à noter que l'étape 14 peut être effectuée avant l'étape 13, ce qui peut selon l'algorithme d'encryptage utilisé rendre encore plus difficile l'accès aux informations mémorisées par la puce 30.

La figure 3 montre les opérations effectuées lors d'un contrôle d'identité d'une personne possédant un support d'identification 10.

10

A l'étape 22, le dispositif de lecture 7 commande le transfert des informations stockées dans la puce transpondeur 30. Ces informations sont ensuite transmises au calculateur 1 pour y être décryptées (étape 23), et analysées de manière à séparer les informations d'identification des informations relatives à l'image numérisée. Les informations d'image sont décompressées (étape 24), puis affichées sur l'écran de visualisation 3 avec les informations d'identification (étape 26). L'opérateur qui effectue le contrôle d'identité peut alors vérifier que les informations imprimées et la photographie figurant sur le support d'identification 10 correspondent bien à celles affichées sur l'écran 3.

15

20

Selon une particularité de l'invention, l'algorithme d'encryptage utilisé est de type à clé d'encryptage, la clé choisie étant le numéro de série de la puce 30 qui est unique et qui est stocké d'une manière inaltérable par les moyens de mémorisation de celle-ci. Les étapes d'encryptage 14 et de décryptage 23 comportent alors une opération préalable de lecture du numéro de série de la puce, à l'aide des moyens de lecture 7.

25

Par ailleurs, on peut prévoir d'automatiser les opérations de vérification en numérisant à l'aide du scanner 2 la photographie 8 apposée sur le support 10 et les informations qui y sont imprimées, et en traitant ces dernières par un logiciel de reconnaissance de caractères (étape 21). Il suffit ensuite d'effectuer à l'étape 27 la comparaison entre les informations lues sur la puce 30 et les informations issues de la numérisation, et d'indiquer sur l'écran d'affichage 3 si des différences ont été détectées.

30

35

Parallèlement, les informations, y compris les données d'image lues dans la puce transpondeur 30 peuvent être comparées aux informations d'identification de

personnes recherchées, stockées dans une base de données 41 accessible au calculateur 1.

Sur la figure 4, la puce transpondeur 30 comprend un module mémoire 34 et un module de transmission 32, le module de transmission étant relié par des moyens de connexion 35 à une antenne 33. L'ensemble des modules mémoire et de transmission peut être fixé sur un support 31 très mince, par exemple en papier. Ainsi, dans le cas d'une puce transpondeur de 16 kbits de capacité mémoire, l'ensemble ne dépasse pas quelques dixièmes de millimètres d'épaisseur. Une telle capacité est parfaitement compatible avec la taille de l'image numérique à stocker, compte tenu des performances actuelles des techniques de compression d'images.

Comme précédemment mentionné, la puce 30 comprend un microprocesseur utilisé pour gérer et contrôler les transferts de données entre la mémoire 34 et le dispositif de lecture et d'écriture 7. Le microprocesseur peut ainsi attribuer une ou plusieurs clés d'accès à l'ensemble ou à certaines parties de la mémoire 34 et bloquer totalement l'accès de la puce après un certain nombre prédéfini de tentatives d'accès à l'aide d'une clé erronée. De cette manière, il n'est pas possible pour une personne non autorisée de copier le contenu d'une puce et de le transférer dans une autre puce.

Le microprocesseur de la puce 30 est également programmé pour gérer les collisions, c'est-à-dire les transmissions simultanées entre un lecteur et plusieurs puces.

Par ailleurs, dans le cas de puces à induction, l'antenne 33 de transmission se présente sous la forme d'une bobine qui permet au dispositif de lecture et/ou d'écriture 7 d'alimenter en énergie par induction la puce 30, le champ magnétique appliqué à la bobine étant modulé pour effectuer la transmission des informations.

La puce transpondeur utilisée par l'invention utilise avantageusement une fréquence de transmission de quelques MHz, de telle sorte que la bobine 33 ne comporte que quelques spires qui peuvent être formées sur le support par un simple procédé d'impression ou de sérigraphie, les moyens de connexion 35 se présentant sous la forme de microbilles déposées directement sur le substrat de silicium de la puce, qui sont soudées aux plots de raccordement de l'antenne

- 7 -

également réalisés par impression ou sérigraphie, la connexion à l'antenne assurant en même temps le maintien de la puce sur le support 10. On peut prévoir en outre de coller une feuille de papier sur le support 10 de manière à recouvrir et masquer l'autre face de la puce 30 et l'antenne 33.

- 5 Alternativement, la puce et son support, ainsi que l'antenne imprimée ou sérigraphiée peut être montée en sandwich entre deux feuilles de papier ordinaire ou sécurisé.

- 10 Il est à noter qu'une telle fréquence de transmission permet d'obtenir un débit de transmission relativement élevé, ce qui permet de réaliser la lecture des informations stockées par la puce presque instantanément.

REVENDEICATIONS

1. Procédé pour l'identification sécuritaire d'une personne, comprenant l'apposition sur un support d'identification (10) du type en papier
5 cartonné ou en matière plastique de faible épaisseur, attribué à la personne, d'informations d'identification de la personne, et la lecture de ces informations, caractérisé en ce qu'il comprend :
- la fixation sur le support d'identification d'une puce électronique (30) de faible épaisseur, comprenant des moyens de mémorisation (34) et des moyens sans
10 contact d'émission et de réception (32) respectivement pour transmettre les informations stockées et pour recevoir les informations à stocker par les moyens de mémorisation,
 - la numérisation (11, 16), puis l'encryptage (14) des informations apposées sur le support d'identification (10),
 - 15 - la transmission (15) sans contact des informations encryptées vers les moyens de réception (32) et leur stockage par les moyens de mémorisation (34), et
 - à chaque identification de la personne, la réception (22) par des moyens de lecture (7) des informations stockées par les moyens de mémorisation (34) de la puce électronique (30) fixée sur le support d'identification (10) attribué à la
20 personne, le décryptage (23) de ces informations, et la comparaison (27) de ces informations avec les informations apposées sur le support d'identification.

2. Procédé selon la revendication 1, caractérisé en ce que les informations d'identification stockées dans la puce
25 électronique (30) comprennent l'image numérisée d'une photographie d'identité (8) et/ou d'une empreinte digitale, le procédé comprenant en outre le traitement (12) de l'image numérisée par un algorithme de compression d'image préalablement à son encryptage (14).

- 30 3. Procédé selon la revendication 1 ou 2, caractérisé en ce que, préalablement à l'encryptage (14) des informations d'identification, il comprend une étape de lecture d'un numéro de série de la puce stocké d'une manière inaltérable par les moyens de mémorisation (34), ce numéro de série étant unique, et l'utilisation de ce numéro de série comme clé
35 d'encryptage, et lors du décryptage (23) des informations stockées par la puce, la lecture préalable de ce numéro de série.

4. Procédé selon l'une des revendications précédentes,

caractérisé en ce que lors de l'identification d'une personne, il comprend la numérisation (21) des informations apposées sur le support, et la comparaison par un calculateur (1) de ces informations avec celles provenant de la puce incorporée dans le support.

5

5. Procédé selon l'une des revendications précédentes, caractérisé en ce que, lors de l'identification d'une personne, il comprend la comparaison des données lues à un ensemble d'informations d'identification de personnes recherchées stocké dans une base de données (41).

10

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que les informations d'identification sont stockées sur la puce (30) selon une organisation prédéfinie qu'il est nécessaire de connaître pour pouvoir lire ces informations.

15

7. Dispositif d'identification d'une personne pour la mise en oeuvre du procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comprend un support (10) en papier ou matière plastique de faible épaisseur, une puce électronique (30) sans contact, dans laquelle sont
20 intégrés des moyens sans contact d'émission et de réception (32) de type transpondeur, et des moyens de mémorisation (34) couplés aux moyens d'émission et de réception et dans lesquels sont stockées les informations d'identification de la personne, les moyens d'émission et de réception comprenant
25 des moyens de connexion (35) pour se connecter à une antenne de transmission (33), l'épaisseur de la puce étant très faible de manière à pouvoir être incorporée au support sans laisser apparaître une surépaisseur importante

30

8. Dispositif selon la revendication 7, caractérisé en ce que la puce (30) est de type à induction, l'antenne (33) de transmission se présentant sous la forme d'une bobine qui permet au dispositif de lecture et/ou d'écriture (7) d'alimenter la puce (30) en énergie par induction, le champ magnétique appliqué à la bobine étant modulé pour effectuer la transmission des informations.

35

9. Dispositif selon la revendication 7 ou 8, caractérisé en ce que la puce (30) utilise avantageusement une fréquence de transmission de quelques MHz, de telle sorte que la bobine (33) ne comporte que quelques spires qui sont formées sur le support par un procédé d'impression, les

1/1

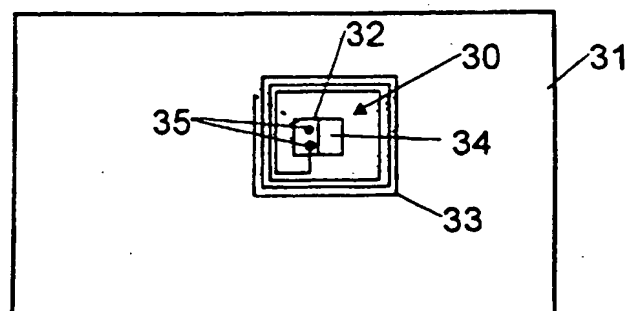
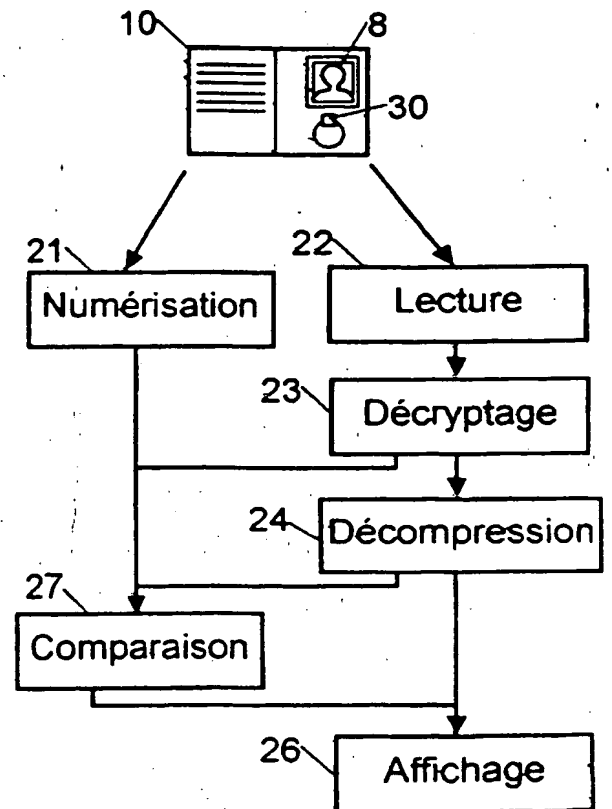
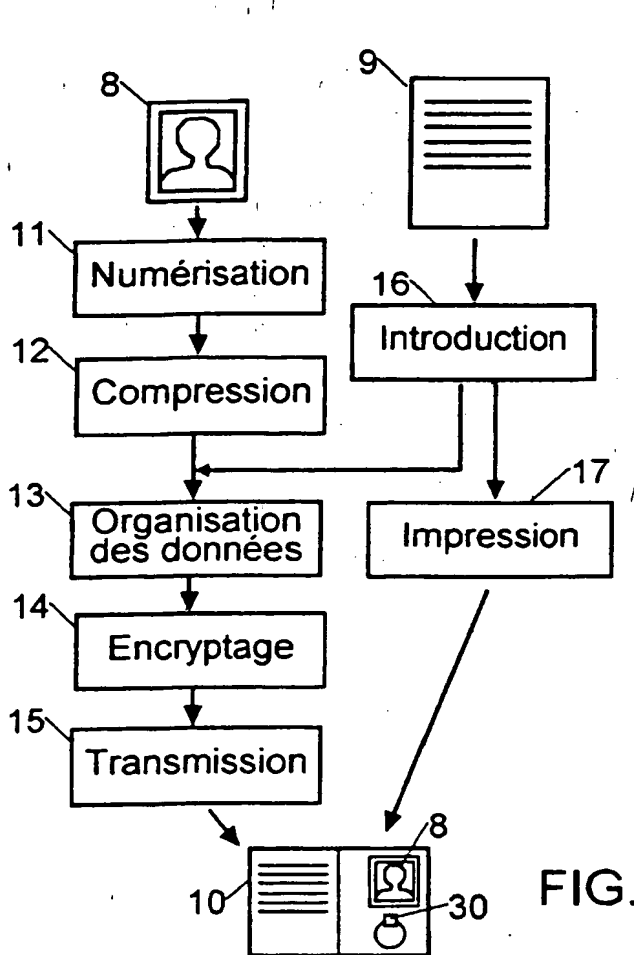
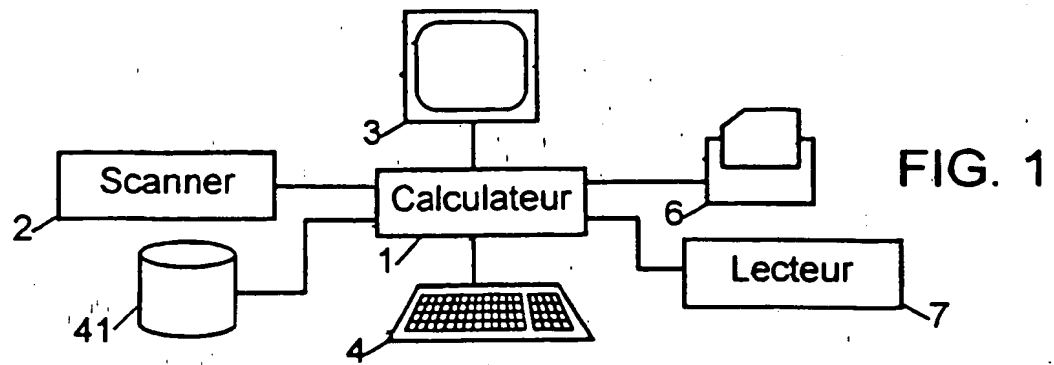


FIG. 4

moyens de connexion (35) se présentant sous la forme de microbilles solidaires de la puce, qui sont soudées sur les bornes de connexion de l'antenne également réalisées par un procédé d'impression, la connexion à l'antenne assurant en même temps le maintien de la puce sur le support (10).

5

10. Dispositif selon l'une des revendications 7 à 9, caractérisé en ce que la puce (30) comprend des moyens de calcul qui n'autorisent l'accès à tout ou partie des moyens de mémorisation (34) que si les moyens d'émission et de réception (32) reçoivent une clé prédéterminée correspondante.

10

11. Dispositif selon l'une des revendications 7 à 10, caractérisé en ce que la puce (30) et l'antenne imprimée sont montées en sandwich entre deux feuilles de papier ordinaire ou sécurisé.

15

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL

de la

PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE

PRELIMINAIRE

établi sur la base des dernières revendications
déposées avant le commencement de la rechercheN° d'enregistrement
nationalFA 557792
FR 9803096

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	US 4 783 823 A (H. TASAKI) 8 novembre 1988 * abrégé; revendications; figures * * colonne 8, ligne 3 - colonne 10, ligne 26 *	1,2,4
Y	US 5 214 699 A (M. MONROE) 25 mai 1993 * abrégé; revendications; figures * * colonne 4, ligne 6 - colonne 5, ligne 31 *	1,2,4 3,6
A	WO 89 12287 A (J-P. TRIPEAU) 14 décembre 1989 * le document en entier *	1,2,4,7, 8,11
A	WO 96 06409 A (GEEFIELD) 29 février 1996 * abrégé; revendications; figures * * page 13, ligne 20 - page 19, ligne 31 *	1-5,7-11
A	EP 0 674 295 A (GEMPLUS CARD INTERNATIONAL) 27 septembre 1995 * le document en entier *	1,2,4
A	GB 2 291 237 A (P.M. ASHKEY) 17 janvier 1996 * abrégé; revendications; figure * * page 9, alinéa 3 *	1,2,4
A	US 4 993 068 A (G.V. PIOSENKA) 12 février 1991	
A	GB 2 173 970 A (MATSUSHITA ELECTRIC WORKS) 22 octobre 1986	
A	WO 93 19942 A (INTELCARD TECHNOLOGIES) 14 octobre 1993	
-/-		
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
		G07F G07C
Date d'achèvement de la recherche		Examineur
19 janvier 1999		David, J
<p>CATÉGORIE DES DOCUMENTS CITÉS</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant</p>		

1

EPO FORM 1503 03.92 (P04C13)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.